



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/587,513

04/25/2007

Toshihisa Nakano

2006\_1239A

2481

52349

7590

03/16/2009

WENDEROTH, LIND & PONACK L.L.P.

1030 15th Street, N.W.

Suite 400 East

Washington, DC 20005-1503

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

03/16/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/587,513	<b>Applicant(s)</b> NAKANO ET AL.	
	<b>Examiner</b> MICHAEL R. VAUGHAN	<b>Art Unit</b> 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 04 February 2009.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

The instant application having Application No. 10/587513 is presented for examination by the examiner. Claims 1, 4, 6, 7, 9, 10, 12, 14, and 17-21 have been amended. Claim 1-21 are pending.

### ***Response to Amendment***

#### ***Specification***

The objection to the specification has been withdrawn due to the amendment.

#### ***Claim Rejections - 35 USC § 101***

The previous 101 rejection has been overcome by the current amendment.

### ***Response to Arguments***

Applicant's arguments filed 2/04/09 have been fully considered but they are not persuasive. Applicant's arguments seem to be grounded in his interpretation of the keys of the Tsuria reference and how they are managed. Examiner has carefully reviewed the submitted arguments but respectfully disagrees that Tsuria does not teach all of the limitations of the claim. In particular, Examiner will respond to the arguments on page 19 in light of claim 1.

Art Unit: 2431

Examiner finds support of converting the generated content in Tsuria. The word convert carries a broad interpretation. Even though Applicant has given the example of converting a file into a low quality version, this limitation is not in the claim. Converting could mean, encrypting, decrypting, re-encrypting, or manner other functions. Tsuria teaches, as one possible interpretation, generating a new key packet which includes the content (0024).

Examiner finds support for the key management of the device key and the medium key of claim 1. Examiner has interpreted device key to be equivalent to Tsuria's key that the first user uses to play the content. The medium key is then the encryption key which the encrypted content is stored on the second user's medium to decrypt the contents. In paragraph 0054-0055 for example, Tsuria teaches that the key packet which is transferred to the second user includes, first user's key [device key], in this case he calls it the original key. In paragraph 0055 the content is re-encrypted or encrypted a second time with a different key. Tsuria teaches that all the keys needed to play the content are sent in the new key packet which has been encrypted with the second user's encryption key. It is inherent that if the encryption key and the content are encrypted by different keys that both of them would be sent to the user, preferably both key encrypted by second user's key, because both are needed to decrypt the content. Tsuria also explicitly teaches the encrypted content (encrypted by the device key) can be encrypted a second time with another key. In this scenario both device key and the other key would still be sent in the new key packet to the second user. Thus

Art Unit: 2431

both the device key and the medium key are sent to the portable medium as the claim reads.

The newly amended limitation which says that the storage unit continues to store the first encrypted content whether or not the device key has been deleted is also suggested by Tsuria. Tsuria mentions in paragraph 0059 that the content may optionally be deleted. He does not say the option depends on whether the device key is deleted or not. Deletion of the content is just that, an option. If one chooses not to delete the first content, it would in fact continue to store it. Tsuria does not teach that the content must be deleted or kept, so that decision is purely up to the application not the presence of the device key.

The other underlying argument is that the Tsuria does not teach or suggest preventing the first device (user) from being able to still play the content once it has transferred the content and rights to a second user. Examiner respectfully disagrees with this assertion. That seems to be the main objective of Tsuria and paragraph 0014-0015 address this objective. The idea of sending the key packet to the second user renders the content unplayable to the first user's device. The basis of DRM is a separation between the content and the right to play it. Without the right to play the content, the content cannot be generated. This prevention of playing is done by not having the correct keys to decrypt the encrypted content.

***Claim Rejections - 35 USC § 102***

Art Unit: 2431

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2004/0030898 to Tsuria et al., hereinafter Tsuria.

As per claim 1, Tsuria teaches a terminal device for transferring a right to use content to a portable medium while protecting a copyright of the content, comprising:

a storage unit storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content (0009);

a decryption unit operable to decrypt the first encrypted content using the device key, to generate the content (0009);

a conversion unit operable to perform an irreversible conversion on the generated content, to generate converted content (0024);

an encryption unit operable to encrypt the converted content using the medium key, to generate second encrypted content (0011 and 0021);

Art Unit: 2431

a write unit operable to move the medium key and the second encrypted content to the portable medium, and read the device key from the storage unit and write the read device key to the portable medium (0011 and 0054-0055); and

a key deletion unit operable to delete the device key from the storage unit (0011 and 0032) thereby preventing the decryption unit from decrypting the first encrypted content (0014)

wherein the storage unit continues to store the first encrypted content irrespective of whether the device key has been deleted or not (0059).

As per claim 2, Tsuria teaches wherein the key deletion unit deletes the device key from the storage unit after the write unit writes the device key to the portable medium (0054), and

the write unit moves the medium key and the second encrypted content to the portable medium after the key deletion unit deletes the device key from the storage unit (0055).

As per claim 3, Tsuria teaches wherein the storage unit further stores key information for encrypting the device key, the encryption unit further encrypts the device key using the key information (0055);

and the write unit writes the encrypted device key to the portable medium, as the device key (0058).

As per claim 4, Tsuria teaches a read unit operable to read the encrypted device key from the portable medium, wherein the decryption unit further decrypts the read

Art Unit: 2431

encrypted device key using the key information to generate the device key, and stores the generated device key to the storage unit (0058).

As per claim 5, Tsuria teaches an embedment unit operable to embed the device key in the converted content, to generate key-embedded content (0055),

wherein the encryption unit encrypts the key-embedded content using the medium key, to generate the second encrypted content (0058),

the key deletion unit deletes the device key from the storage unit after the embedment unit embeds the device key in the converted content (0059), and

the write unit moves the medium key and the second encrypted content to the portable medium after the key deletion unit deletes the device key from the storage unit (0060).

As per claim 6, Tsuria teaches an extraction unit operable to extract the device key from the key-embedded content, and store the extracted device key to the storage unit, wherein a read unit reads the second encrypted content and the medium key from the portable medium (0061), and

the decryption unit further decrypts the read second encrypted content using the read medium key to generate the key-embedded content, and outputs the generated key-embedded content to the extraction unit (inherent that the 2nd device is able to read the newly received encrypted data as evidenced by its ability to repeat the process to a third device).



Art Unit: 2431

As per claim 7, Tsuria teaches a read unit operable to read the device key from the portable medium, wherein the read unit stores the read device key to the storage unit (0060).

As per claim 8, Tsuria teaches a reproduction unit operable to reproduce the content, wherein the decryption unit further reads the first encrypted content and the device key from the storage unit, decrypts the read first encrypted content using the read device key to generate the content, and outputs the generated content to the reproduction unit (0013).

As per claim 9, Tsuria teaches a content protection system for transferring a right to use content from a terminal device to a portable medium while protecting a copyright of the content, the terminal device comprising:

- a first storage unit storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content (0009);
- a decryption unit operable to decrypt the first encrypted content using the device key, to generate the content (0009);

- a conversion unit operable to perform an irreversible conversion on the generated content, to generate converted content (0021);

- an encryption unit operable to encrypt the converted content using the medium key, to generate second encrypted content (0011 and 0021);

- a write unit operable to move the medium key and the second encrypted content to the portable medium, and read the device key from the first storage unit and write the read device key to the portable medium (0011); and

Art Unit: 2431

a key deletion unit operable to delete the device key from the first storage unit, and the portable medium comprising (0011) thereby preventing the decryption unit from decrypting the first encrypted content (0014)

a second storage unit operable to store the device key, the medium key, and the second encrypted content received from the terminal device (0017),

wherein the key deletion unit deletes the device key from the first storage unit after the write unit writes the device key to the second storage unit (0054), and

the write unit moves the medium key and the second encrypted content to the portable medium after the key deletion unit deletes the device key from the first storage unit (0055) wherein the storage unit continues to store the first encrypted content irrespective of whether the device key has been deleted or not (0059).

As per claim 10, Tsuria teaches wherein the terminal device further comprises: a read unit operable to read the device key from the second storage unit, the read unit stores the read device key to the first storage unit, the portable medium further comprises:

a deletion unit operable to delete at least one of the second encrypted content and the medium key from the second storage unit, and

the read unit reads the device key from the second storage unit after the deletion unit deletes the at least one of the second encrypted content and the medium key from the second storage unit (0059-0061). It is inherent that the receiving terminal can reverse the encryption process to generate content. The terminal both reads and writes

Art Unit: 2431

to the portable medium. Therefore it is able to perform sending and receiving which are reciprocal processes to one another.

As per claim 11, Tsuria teaches wherein the first storage unit further stores key information for encrypting the device key (0051),

the encryption unit further encrypts the device key using the key information,

the write unit writes the encrypted device key to the second storage unit as the device key, and after writing the encrypted device key, moves the medium key and the second encrypted content to the second storage unit (0057), and

the second storage unit stores the encrypted device key as the device key (0058).

As per claim 12, Tsuria teaches wherein the terminal device further comprises: a read unit operable to read the encrypted device key from the second storage unit, wherein the decryption unit further decrypts the read encrypted device key using the key information to generate the device key, and stores the generated device key to the first storage unit (0058), the portable medium further comprises:

a deletion unit operable to delete at least one of the second encrypted content and the medium key from the second storage unit, and

the read unit reads the encrypted device key from the second storage unit after the deletion unit deletes the at least one of the second encrypted content and the medium key from the second storage unit (0059-0061). It is inherent that the receiving terminal can reverse the encryption process to generate content. The terminal

Art Unit: 2431

both reads and writes to the portable medium. Therefore it is able to perform sending and receiving which are reciprocal processes to one another.

As per claim 13, Tsuria teaches an embedment unit operable to embed the device key in the converted content, to generate key-embedded content (0055),

the encryption unit encrypts the key-embedded content using the medium key, to generate the second encrypted content (0058),

the key deletion unit deletes the device key from the first storage unit after the embedment unit embeds the device key in the converted content (0059), and

the write unit writes the medium key and the second encrypted content to the second storage unit after the key deletion unit deletes the device key from the first storage unit (0060).

As per claim 14, Tsuria teaches the terminal device further comprises:  
an extraction unit operable to extract the device key from the key-embedded content, and store the extracted device key to the first storage unit,

a read unit reads the second encrypted content and the medium key from the second storage unit,

the decryption unit further decrypts the read second encrypted content using the read medium key to generate the key-embedded content, and outputs the generated key-embedded content to the extraction unit (inherent that the 2nd device is able to read the newly received encrypted data as evidenced by its ability to repeat the process to a third device), and

Art Unit: 2431

the portable medium deletes the second encrypted content and the medium key from the second storage unit after the terminal device reads the second encrypted content and the medium key from the second storage unit (0061).

As per claim 15, Tsuria teaches a mobile information terminal, wherein the mobile information terminal reads, from the portable medium in which the device key, the medium key, and the second encrypted content are stored in the second storage unit, the second encrypted content and the medium key, decrypts the read second encrypted content using the read medium key to generate the converted content, and reproduces the converted content (0060).

As per claim 16, Tsuria teaches another terminal device connected with the terminal device,

wherein the another terminal device comprises: a read unit operable to read, from the portable medium in which the device key, the medium key, and the second encrypted content are stored in the second storage unit, the device key, the medium key, and the second encrypted content (0059);

a deletion unit operable to delete at least one of the medium key and the second encrypted content read by the read unit; and

an acquisition unit operable to acquire the first encrypted content from the terminal device, after the deletion unit deletes the at least one of the medium key and the second encrypted content, the portable medium moves the device key, the medium key, and the second encrypted content to the another terminal device (0060), and

the terminal device further comprises:

Art Unit: 2431

a transmission unit operable to transmit the first encrypted content to the another terminal device; and a content deletion unit operable to delete the first encrypted content from the first storage unit (0061).

As per claim 17, Tsuria teaches a portable medium for receiving a right to use content from a terminal device while protecting a copyright of the content, the terminal device including: a storage unit storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content; a decryption unit operable to decrypt the first encrypted content using the device key, to generate the content; a conversion unit operable to perform an irreversible conversion on the generated content, to generate converted content; an encryption unit operable to encrypt the converted content using the medium key, to generate second encrypted content; a write unit operable to move the medium key and the second encrypted content to the portable medium, and read the device key from the first storage unit and write the read device key to the portable medium; and a key deletion unit operable to delete the device key from the first storage unit (0049-0050) wherein the storage unit continues to store the first encrypted content irrespective of whether the device key has been deleted or not (0059), the portable medium comprising:

a storage unit operable to store the device key, the medium key, and the second encrypted content (0051).

As per claim 18, Tsuria teaches a content movement method used in a terminal device for transferring a right to use content to a portable medium while protecting a copyright of the content, the terminal device storing first encrypted content, a device

Art Unit: 2431

key, and a medium key, the first encrypted content being generated by encrypting the content (0009), the content movement method comprising:

- a decryption step of decrypting the first encrypted content using the device key, to generate the content (0009);

- a conversion step of performing an irreversible conversion on the generated content, to generate converted content (0011);

- an encryption step of encrypting the converted content using the medium key, to generate second encrypted content (0011 and 0021);

- a write step of moving the medium key and the second encrypted content to the portable medium, and reading the device key from the storage unit and writing the read device key to the portable medium (0021); and

- a key deletion step of deleting the device key from the terminal device (0021).

As per claim 19, Tsuria teaches wherein the key deletion step deletes the device key from the terminal device after the write step writes the device key to the portable medium (0054), and the write step moves the medium key and the second encrypted content to the portable medium after the key deletion step deletes the device key from the terminal device (0058).

As per claim 20, Tsuria teaches a content movement program used in a terminal device for transferring a right to use content to a portable medium while protecting a copyright of the content, the terminal device storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content (0009), the content movement method comprising:

a decryption step of decrypting the first encrypted content using the device key, to generate the content (0009);

a conversion step of performing an irreversible conversion on the generated content, to generate converted content (0011);

an encryption step of encrypting the converted content using the medium key, to generate second encrypted content (0011 and 0021);

a write step of moving the medium key and the second encrypted content to the portable medium, and reading the device key from the storage unit and writing the read device key to the portable medium (0021); and

a key deletion step of deleting the device key from the terminal device (0021).

As per claim 21, Tsuria teaches wherein the key deletion step deletes the device key from the terminal device after the write step writes the device key to the portable medium (0054), and the write step moves the medium key and the second encrypted content to the portable medium after the key deletion step deletes the device key from the terminal device (0058) wherein the storage unit continues to store the first encrypted content irrespective of whether the device key has been deleted or not (0059).

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP



Art Unit: 2431

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

Art Unit: 2431

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431